SECURIT-e-DOC®

Securit-e-Doc®
SITT® CryptoSystem

FIPS 140-1 Non-Proprietary Security Policy

Level 1 Validation

September 26th, 2002
Version 1.3

Table of Contents

1 Introduction

1.1 Purpose

This is a security policy produced for compliance to Federal Information Processing Standard Publication 140-1 (FIPS PUB 140-1). This security policy was prepared for the level 1 validation of Securit-e-Doc's Secure Information Transport Technology (*SITT*®) Cryptosystem. This document describes how the Securit-e-Doc SITT® Cryptosystem meets all FIPS 140-1 requirements.

1.2 References

For more information about Securit-e-Doc and their products, please visit:

http://www.securit-e-doc.com/

For more information about Federal Information Processing Standard Publication 140-1 please refer to NIST's website at:

http://csrc.nist.gov/cryptval/

1.3 Document Organization

The Security Policy document is one document in the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This Security Policy and other Validation Submission Documentation was produced by Corsec Security, Inc. under contract to Securit-e-Doc, Inc. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Validation Submission Documentation is Securit-e-Doc - proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Securit-e-Doc, Inc.

2 Securit-e-Doc

Securit-e-Doc is a complete e-document delivery & storage solution powered by the SITT® Cryptosystem. The concept behind Securit-e-Doc is to enable secure communication via automated protection of data in transit and while in storage. The implementation goal was to do it transparently to the user, and make it simple; but to build it with the best that mathematics and science have to offer in proven cryptographic algorithms.

The result, after years of development, is Securit-e-Doc's new family of software, powered by the SITT® delivery engine, an automated cryptosystem engineered for today's serious information security requirements. Securit-e-Doc, Inc. has produced a fully web-enabled, totally interactive, point-to-point secure message and document communication, called S-Doc 3.0.

2.1 SITT®

Securit-e-Doc, Inc. has developed and filed a patent for its Secure Information Transport Technology (*SITT*®), an encryption delivery engine that has the potential to set a new standard in securing the storage and transport of digital information. The essence of *SITT*® is a one-time, customizable, server-generated and delivered encryption process that requires little more than an Internet browser on any device connected to the Web. Securit-e-Doc, Inc. expects to apply this advanced technology to all areas where digital information needs to be securely stored, transported, and delivered over the Internet or intranets.

Securit-e-Doc provides secure transmission and storage of documents using web-enabled interfaces. Securit-e-Doc consists of a server application, clientless access through the web, and a downloaded client interface. All components of the Securit-e-Doc system derive their security services from the underlying SITT®. The system makes use of web servers running Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to secure initial communications.

SITT® sits under the Securit-e-Doc application software and provides cryptographic services for symmetric encryption and decryption, random number generation, and message digesting.

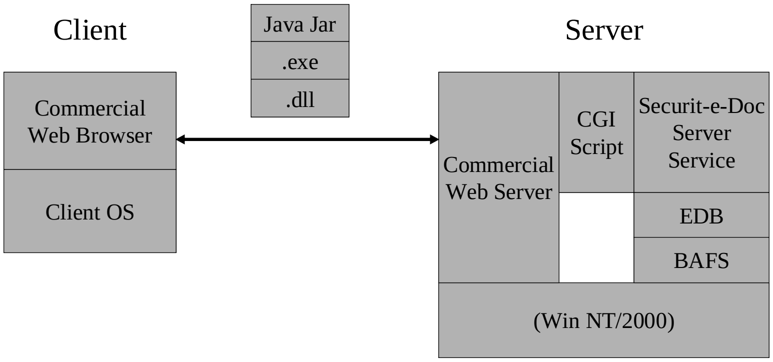

Figure 1 – Overall Securit-e-Doc Architecture

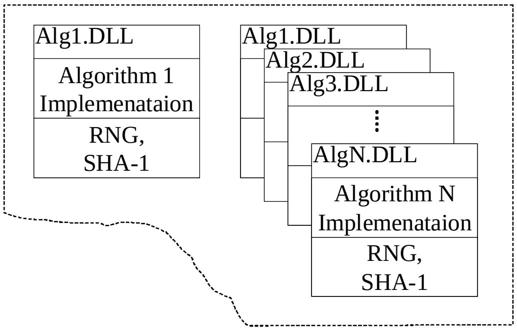

Figure 2 – SITT® Cryptosystem Components

There are multiple components to the SITT® Cryptosystem, each consisting of a distinct and separate implementation of a Dynamic Link Library (DLL). Each DLL shares a common architecture, Finite State Machine (FSM) model, FIPS 140-1-compliant random number generator, and message digesting algorithm. The SITT® Cryptosystem consists of three separate algorithm DLLs that implement three separate FIPS 140-1 compliant symmetric algorithms. See section 2.5 for a description of supported FIPS-compliant algorithms. The SITT® Cryptosystem only contains FIPS approved techniques and only has one operational mode, which is FIPS approved.

When a Federal Government customer installs Securit-e-Doc's e-document delivery & storage solution, the server installation process requires algorithm selection. Federal Government customers are only offered and must select the FIPS approved algorithms, which selects the FIPS 140-1 validated SITT® Cryptosystem. See section 2.5 for algorithm options. Once the server is installed these implanted algorithms cannot be changed, enforcing use of FIPS-validated algorithms for all server and client component uses system-wide. The SITT crypto-system is a closed system as the encryption process is fully automated and not subject to user controls. The module is not used as a server, however the module's cryptographic functions can be called by a server.

2.2 Interfaces, Roles, and Services

SITT® is designed to provide cryptographic services to a single user or application making use of the validated cryptographic functions. As allowed by FIPS 140-1 for level 1 cryptographic modules, identification and authentication of operators is not implemented. Operators of the module implicitly assume one of the two supported roles when calling functions associated with that role. The two roles supported are Crypto Officer (to load the module and run the self-tests), and the User role to exercise cryptographic functions.

The module provides an Application Programming Interfaces (APIs) to export cryptographic functions to calling applications. Each individual algorithm DLL exports the same generic interface, which includes the following functions:

- DLLMain() (This is the main module initialization function, loading up the software and performing self-test. This is a Crypto-Officer-role function)
- Symmetric Encryption (User-role functions)
    - __encdecbuf(); This function provides a generic pointer to encdecbuf().

    - encdecbuf(); This function performs symmetric encryption on a pre allocated buffer of data.
    - encdecFILE(); This function performs symmetric encryption on a file.
    - keysz(); This function is used to return the symmetric key size expected for encryption calls.
- Hashing functions (User-role functions)
    - sha1raw(); This function is used to perform SHA-1 hashing on raw data streams.
    - sha1buf(); This function is used to perform SHA-1 hashing of fixed lengths of preallocated data
    - key_expand(); This function performs buffer expansion, spreading a supplied value over a supplied buffer using hashing.
    - key_plus_entropy();This function calls key_expand after adding in random data to the supplied value.
- FIPS 140-1 compliant random number generation (User-role functions)
    - *prng_name[]This function returns a list of supported pseudo random number generation function names.
    - *prng_alg[] This function returns pointers to a supported pseudo random number generation functions based on function name.
    - ctx186_init(); This function initializes a random number generator structure and allocated memory for it.
    - ctx186_free(); This function destroys a random number generator structure and de-allocates the memory for it.
    - ctx186_fill(); This function performs continuous random number generation self tests, computes random numbers and stores them for use as requested by ctx186_rand()
    - ctx186_rand(); This function provides random numbers, calling ctx186_fill() if necessary to compute additional random numbers.

2.3 Software, Physical, EMI/EMC, and Operating System Security

The Securit-e-Doc SITT® Cryptosystem is a software module and was tested on the Windows 2000 operating system. The SITT® module can also be operated upon other Windows-compatible platforms, but was not tested upon these platforms. The module was tested against FIPS 140-1 requirements on a standard Intel platform Personal Computer (PC) that meets all FIPS 140-1 level 1 physical requirements. This includes providing production grade equipment, standard passivation of components, and FCC certification against electromagnetic interference and compatibility.

2.4 Cryptographic Key Management

SITT® allows users to manage keys, importing and exporting symmetric keying material through the API calls provided to the User role. Internally to the module, symmetric keys are used to perform operations and then actively zeroized after completion of the operation. Keys are not stored by the module, with the exception of keys used by the module to implement internal self-tests. This triple-DES key is installed with the module, and destroyed with deletion of the module.

2.5 *Cryptographic Algorithms*

SITT® supports several cryptographic algorithms to perform encryption and decryption, message digesting, and random number generation. The following FIPS-approved algorithms are supported:

Encryption Algorithms:

- **Skipjack** as referenced in FIPS 185, *Escrowed Encryption Standard (EES)*, and specification in SKIPJACK and KEA Algorithm Specifications *(Version 2.0, 29 May 1998)*.
- **Advanced Encryption Standard** (AES) Cyclic Block Chaining (CBC) as specified in FIPS 197, *Advanced Encryption Standard.*
- **Triple DES** Cyclic Block Chaining (CBC) mode as specified in FIPS 46-3, *Data Encryption Standard (DES)*, and ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation.*

Message Digesting Algorithm:

- **Secure Hash Algorithm** (SHA-1) as specified in FIPS 180-1, *Secure Hash Standard (SHS).*

2.6 *Self-Tests*

All components of the Securit-e-Doc SITT® Cryptosystem perform self-tests to ensure correct operation, both at startup and conditionally where required. Each DLL performs and computes a Message Authentication Code (MAC) as defined in FIPS 113, *Computer Data Authentication*, using Triple DES to ensure the DLL has not been corrupted. Additionally, all cryptographic algorithms perform known answer tests testing correct operation of the symmetric encryption algorithms and SHA-1 hashing.

The module implements a FIPS 140-1 compliant random number generator from FIPS 186-2, and includes a continuous random number generator test to prevent failure to a constant value.

3 Acronym List

API **Application Program Interface**
A set of defined function calls provided by an executable, library, or device.

CBC **Cipher Block Chaining**
A mode of symmetric block encryption whereby each block of cipher-text created is exclusive-or-ed with the next block of plain-text before encryption. CBC mode avoids encryption of repeated plain-text blocks to the same cipher-text blocks in a stream of data. CBC mode requires the use of an initialization vector (IV) to exclusive-or with the first block of plaintext data.

DES **Data Encryption Standard**
A FIPS-approved symmetric-key encryption algorithm, specified in FIPS 46-3, *Data Encryption Standard*

DLL **Dynamic Link Library**
A compiled set of executable functions and data that can be accessed by other applications running on a Windows operating system. DLL normally have a .dll, .exe, or .fon extension, and export functions for programs to access through static or dynamic links to the DLL. Static links persist during program execution while a dynamic link are created and destroyed by the program as needed.

EMC **Electromagnetic Compatibility**

A cryptographic module should conform to the EMI/EMC requirements specified by FCC Part 15, Subpart J, Class A (i.e., business use) for Security Levels 1 and 2; for Security Levels 3 and 4, the module must meet Class B (home use) requirements

EMI **Electromagnetic Interference**

A cryptographic module should conform to the EMI/EMC requirements specified by FCC Part 15, Subpart J, Class A (i.e., business use) for Security Levels 1 and 2; for Security Levels 3 and 4, the module must meet Class B (home use) requirements

FIPS 140-1 **Security Requirements for Cryptographic Modules**

Specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. [from the FIPS 140-1 Standard]

FIPS PUB **Federal Information Processing Standard Publication**

A standard published by NIST; there are many Federal Information Processing Standard Publications including:

- FIPS 46-3 and 81 *Data Encryption Standard (DES)* and *DES Modes of Operation*. FIPS 46-3 specifies the DES and Triple DES algorithms
- FIPS 140-1: *Security Requirements for Cryptographic Modules*
- FIPS 171: *Key Management Using ANSI X9.17*
- FIPS 185: *Escrowed Encryption Standard (EES)*, which specifies the Skipjack algorithm
- FIPS 186-2 and FIPS 180-1: *Digital Signature Standard (DSS)* and *Secure Hash Standard (SHS)*, which specify the DSA, RSA, ECDSA, and SHA-1 algorithms

FSM **Finite State Machine**

A document required for FIPS 140-1 validation that contains a diagram and descriptive tables of specific states of the module and transitions in and out of each state; detailed requirements are in section 4 of the Vendor Evidence document

KEA **Key Exchange Algorithm**

A key exchange algorithm using public key cryptography to protect and exchange symmetric encryption keys. KEA is defined with Skipjack in FIPS 185, *Escrowed Encryption Standard.*

MAC **Message Authentication Code**

A symmetric encryption algorithm based digital signature scheme defined in FIPS 113, *Computer Data Authentication.*

NIST **National Institute of Standards and Technology**

A non-regulatory federal agency within the Department of Commerce's Technology Administration that oversees NVLAP and issues certificates for FIPS evaluations (both cryptographic module and algorithm evaluations)

PC **Personal Computer**

An abbreviation for any general-purpose desktop computer.

SHA **Secure Hash Algorithm**

Currently the only FIPS-approved method for secure hashing; details specified in FIPS 180-1. Also referred to as SHA-1 to distinguish it from the predecessor standard FIPS 180.

SHS **Secure Hash Standard**

FIPS PUB 180-1, *Secure Hash Standard*, specifying the SHA-1 algorithm.

SSL **Secure Sockets Layer**

An Internet Engineering Task Force (IETF) approved standard (originally developed by Netscape) specifying a protocol for establishing secure, authenticated communications between web browsers and web servers.

TLS **Transport Layer Security**

A protocol providing a standards based successor to SSL, and also providing negotiated, secure, authenticated communications between web browsers and web servers.